ICS 35.080
L 77

中华人民共和国国家标准

GB/T 25000.51—2016
代替 GB/T 25000.51—2010

系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第51部分:就绪可用软件产品(RUSP)的质量要求和测试细则

**Systems and software engineering—
Systems and software Quality Requirements and
Evaluation (SQuaRE)—Part 51: Requirements for quality of Ready to
Use Software Product (RUSP) and instructions for testing**

(ISO/IEC 25051:2014,Software engineering—
Systems and software Quality Requirements and Evaluation (SQuaRE)—
Requirements for quality of Ready to Use Software Product (RUSP)
and instructions for testing,MOD)

2016-10-13 发布　　2017-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前言 …… Ⅲ
引言 …… Ⅴ
1　范围 …… 1
2　符合性 …… 2
3　规范性引用文件 …… 2
4　术语和定义、缩略语 …… 2
4.1　术语和定义 …… 2
4.2　缩略语 …… 5
5　RUSP 的要求 …… 5
5.1　产品说明要求 …… 5
5.2　用户文档集要求 …… 8
5.3　软件质量要求 …… 10
6　测试文档集要求 …… 13
6.1　一般要求 …… 13
6.2　测试计划要求 …… 14
6.3　测试说明要求 …… 15
6.4　测试结果要求 …… 15
7　符合性评价细则 …… 16
7.1　一般原则 …… 16
7.2　符合性评价先决条件 …… 17
7.3　符合性评价活动 …… 17
7.4　符合性评价过程 …… 17
7.5　符合性评价报告 …… 17
7.6　后续符合性评价 …… 18
附录 A（资料性附录）　业务或安全攸关的应用系统中的 RUSP 的评价指南 …… 19
附录 B（资料性附录）　如何使用本部分 …… 22
参考文献 …… 23

前　言

GB/T 25000《系统与软件工程　系统与软件质量要求和评价(SQuaRE)》分为如下几部分:

——第1部分:SQuaRE指南;
——第2部分:计划与管理;
——第10部分:系统与软件质量模型;
——第12部分:数据质量模型;
——第20部分:测量参考模型和指南;
——第21部分:质量测度元素;
——第22部分:使用质量测量;
——第23部分:系统和软件产品质量测量;
——第24部分:数据质量测量;
——第30部分:质量需求;
——第40部分:评价过程;
——第41部分:开发方、需方和独立评价方的评价指南;
——第42部分:评价模块;
——第45部分:可恢复性的评价模块;
——第51部分:就绪可用软件产品(RUSP)的质量要求和测试细则;
——第60部分:易用性测试报告行业通用格式(CIF):易用性相关信息的通用框架;
——第62部分:易用性测试报告行业通用格式(CIF);
——第63部分:易用性的行业通用格式(CIF):使用周境描述;
——第64部分:易用性的行业通用格式(CIF):用户要求报告;
——第65部分:易用性的行业通用格式(CIF):用户需求规格说明;
——第66部分:易用性的行业通用格式(CIF):评价报告。

本部分为GB/T 25000的第51部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 25000.51—2010《软件工程　软件产品质量要求和评价(SQuaRE)　商业现货(COTS)软件产品的质量要求和测试细则》。与GB/T 25000.51—2010相比,主要技术变化如下:

a) GB/T 25000.51—2010等同采用ISO/IEC 25051:2006,本部分修改采用ISO/IEC 25051:2014。
b) 术语和定义作了调整和补充。
c) 本部分中增加了“信息安全性”和“兼容性”的有关产品质量特性的表述,使用质量特性调整为“有效性”、“效率”、“满意度”、“抗风险”和“周境覆盖”5大特性,相关的子特性也做了修改、调整和补充(增加的条款详见5.1.2.1、5.1.4、5.1.6.2、5.1.6.3、5.1.8.4、5.1.10、5.1.15、5.1.16、5.1.17、5.2.13.1、5.2.15.1、5.2.16.1、5.2.17、5.2.18.1、5.2.19.1、5.3.3、5.3.4.1、5.3.5.5、5.3.6.1、5.3.7.1、5.3.9、5.3.10、5.3.11、5.3.12、5.3.13、6.2.4、6.2.5、6.2.6、6.2.7)。
d) 附录部分也作了调整。

本部分采用重新起草法修改采用ISO/IEC 25051:2014《软件工程　系统与软件质量要求和评价(SQuaRE)　就绪可用软件产品(RUSP)的质量要求和测试细则》(英文版)。本部分与ISO/IEC 25051:2014的主要技术差异及其原因如下:

a) 规范性引用文件中将原国际标准中引用的ISO/IEC 25000删去,因为正文中未引出;将ISO/IEC 25010替换为注日期引用的国家标准GB/T 25000.10—2016,因为质量模型的引用必定是注日期引用。

b) 由于 GB/T 25000.10—2016 是修改采用 ISO/IEC 25010:2011,据此 5.1、5.2、5.3 的相关特性说明做了相应修改,主要针对依从性问题。

c) 国际标准中 5.1.4.1“产品说明中描述的全部功能,应依照软件质量特性的要求进行分类(5.3.2～5.3.9)”纠正为“产品说明中描述的全部功能,宜按照软件产品质量特性的说明进行归类(5.1.5～5.1.12)”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位:中国电子技术标准化研究院、上海计算机软件技术开发中心、国家应用软件产品质量监督检验中心、广东省科技基础条件平台中心、深圳市中安测标准技术有限公司、佛山柯维光电股份有限公司、重庆市软件评测中心有限公司、南京大学、珠海南方软件网络评测中心、湖北软件评测中心、中国航天科技集团公司软件评测中心、内蒙古电子信息产品质量检验院、南昌金庐软件园软件评测培训有限公司、上海泽众软件科技有限公司、上海得元信息科技有限公司、上海市软件行业协会。

本部分起草人:张旸旸、冯惠、蔡立志、胡芸、王威、丁晓明、宋红波、罗亮、潘宇聪、何志明、廖辉、张毅、薛保平、徐宝文、侯建华、王瑞、杨桂枝、夏启铭、黄兆森、刘潇健、李晓春、丁为清、高海龄、巩韶飞、张雪莉、陈海、李英华。

本部分所代替标准的历次版本发布情况为:

——GB/T 17544—1998;

——GB/T 25000.51—2010。

引　言

就绪可用软件产品(RUSP)的应用领域不断拓广,其正确的运行对于业务、安全或个人的应用往往至关重要。

RUSP 可以是一种打包出售给对其特征和其他质量没有任何影响的需方的软件产品。典型情况是,这种软件产品与其用户文档集一起预先包装好出售,或者从 Web 商店下载。用户能在任何时间通过云计算使用的软件产品可以认为是 RUSP。包装封面提供的信息或者供方网站上的信息往往是制造商或营销组织能与需方或用户交流的唯一手段。因此,给出基本信息,使需方能按自己需要来评价 RUSP 的质量是重要的。

由于 RUSP 可能要在各种环境中运行,并且用户没有机会就所选择的产品与类似产品作性能比较,因此选用高质量的 RUSP 是极其重要的。供方需要一种方式来确保用户信任 RUSP 提供的服务。一些供方可能选择符合性评价组织的评价或认证,以协助其提供这种信任。

此外,当用户要求提供涉及业务或安全攸关风险的保证时,这种保证可能需要由用户在采购后选用特定的技术来处置。本部分不规定 RUSP 的最低限度的业务或安全攸关的质量要求,但给出了资料性指南(参见附录 A)。

系统与软件工程　系统与软件质量要求和评价(SQuaRE)　第51部分:就绪可用软件产品(RUSP)的质量要求和测试细则

1　范围

GB/T 25000 的本部分确立了:

a)　就绪可用软件产品(RUSP)的质量要求;

b)　用于测试 RUSP 的包含测试计划、测试说明和测试结果等的测试文档集要求;

注 1:用于测试的文档的汇集称为“测试文档集”。

c)　RUSP 的符合性评价细则。

本部分还包括关于安全或业务攸关的 RUSP 的建议。

本部分仅涉及向用户提供对产品的信任,即 RUSP 能按所提供的和交付的说明运行。不涉及生产实现(包含各种活动和中间产品,例如规格说明)。供方的质量体系超出了本部分的范围。

本部分适用于 RUSP。

注 2:RUSP 的例子包括但不限于:文本处理程序、电子表格、数据库控制软件、图形包、以及用于技术的、科学的或实时的嵌入式功能的软件(例如实时操作系统)、人力资源管理软件、销售管理、智能手机应用、免费软件以及诸如 Web 网站和主页生成器之类的 Web 软件。

注 3:开源软件不属于 RUSP 的范畴。

本部分的预期用户包括:

a)　供方,当:

1)　规定 RUSP 的需求时;

2)　对照所声称的特性评估其软件产品时;

3)　发布符合性声明[ISO/IEC 17050]时;

4)　申请符合性证书或标志[ISO/IEC 导则 23]时;

b)　希望建立某种认证模式(国际级、地区级或国家级)[ISO/IEC 导则 28]的认证机构;

c)　遵循本测试细则提供符合性证书或标志而进行测试的测试实验室[ISO/IEC 17025];

d)　认可注册机构或认证机构以及测试实验室的认可机构;

e)　潜在的需方,其可能:

1)　把预期的工作任务要求与现有软件产品的产品说明信息进行比较;

2)　寻求已获认证的 RUSP;

3)　检验要求是否被满足;

f)　可从更好的软件产品获益的最终用户;

g)　正在进行以下活动的组织:

1)　根据本部分的质量要求和方法建立管理和工程环境;

2)　管理和改进其质量过程及人力资源配置;

h)　可能对安全或业务攸关的应用中使用的 RUSP 提出要求或推荐使用本部分的要求的监管机构。

附录 B 给出了如何使用本部分的参考信息。

2 符合性

RUSP 满足以下条件即符合本部分：

a) 具有第 5 章中规定的特性；

b) 已按所编制的符合第 6 章要求的测试文档集进行了测试；

c) 记录测试期间发现的异常，并在产品发布前解决了这些异常。应消除违背广告宣传的性能声称的异常，否则应取消此种性能声称。如果存在下述两种情况，可认为已知的异常是可接受的：

   1) 该异常不违背所声称的性能；

   2) 供方已适当考虑了该异常的性质和对潜在需方的影响，认为该异常可忽略不计，并且已保存了有关这些异常的文档以备日后改进。

第 7 章和附录 A 是可选的。

注： 为便于符合性评价，本部分的要求是以第 3 级子条方式给出的(编号为 X.X.X.X)。资料性注释完善这些条款，可以作为指南。

3 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第 10 部分：系统与软件质量模型

4 术语和定义、缩略语

4.1 术语和定义

下列术语和定义适用于本文件。

4.1.1

需方 acquirer

从供方获取或采购产品或服务的利益相关方。

注： 需方可能是以下之一：买主、顾客、拥有者、采购者。

[ISO/IEC 12207:2008]

4.1.2

异常 anomaly

与基于需求规格说明、设计文档和标准等的期望值的偏离或与某个人的感知或经验的任何条件的偏离。

[IEEE std 1044—2009]

4.1.3

应用管理职能 application administration function

由用户履行的职能，包括安装、配置、备份、维护(打补丁和升级)、卸载等。

4.1.4

符合性评价 conformity evaluation

对产品、过程或服务达到规定要求的程度所进行的系统性考核。

[ISO/IEC 导则 2:2004]

4.1.5

符合性评价报告　conformity evaluation report

说明对 RUSP 实施评价的行为和结果的文档。

注：改写 IEEE std 610.12—1998。

4.1.6

就绪可用软件产品　Ready to Use Software Product

RUSP

无论是否付费，任何用户可以不经历开发活动就能获得的软件产品。

注 1：RUSP 包括：

——产品说明（包括全部封面信息、数据表、网页信息等）；

——用户文档集（安装和使用软件所必需的文档），包括为运行该软件产品所要求的操作系统或目标计算机的任何配置；

——计算机媒体（磁盘、CD-ROM、网络可下载的媒体等）上的软件。

注 2：软件主要由程序和数据组成。

注 3：本定义也适用于产品说明、用户文档集，以及作为单独的制成品而被生产和支撑的软件，该软件不收取通常的商业费用和证书费用。

4.1.7

最终用户　end user

最终受益于 RUSP 功能的个人。

注：最终用户可以是软件产品的正式操作员；或是临时用户，例如公众中的一员。

[GB/T 25000.1—2010，定义 4.14]

4.1.8

故障　fault

计算机程序中不正确的步骤、过程或数据定义。

[IEEE std 610.12—1998]

4.1.9

维护　maintenance

在交付后对软件系统进行修改的过程。

注：目的是更正错误、改进性能和属性、适应环境等。

[IEEE std 610.12—1998]

4.1.10

通过/失败准则　pass/fail criteria

用于确定软件项或软件特征是否通过测试的判定准则。

[IEEE std 829.12—1998]

4.1.11

产品说明　product description

陈述软件各种性质的文档。

注：主要目的是帮助潜在的需方在采购前对软件本进行适用性评价。

4.1.12

产品标识　product identification

软件产品的名称、版本、变体和日期信息。

4.1.13

需求文档　requirements document

包含 RUSP 要满足的要求或规则的任何组合的文档。

注：这些文档可以是技术报告、标准、针对某类用户的要求列表（或模型需求规格说明）或者是行政机构或管理机构颁发的条例或法规。

4.1.14

软件功能　software function

软件中算法的实现，利用该实现，最终用户或软件可以执行某一工作任务的部分或全部。

注：功能不一定是最终用户可调用的（例如：数据的自动备份保存）。

4.1.15

软件测试环境　software test environment

对软件进行合格性测试或其他测试时所需要的设施、硬件、软件、固件、规程和文档集等。

[ISO/IEC/IEEE 24765:2010]

4.1.16

供方　supplier

与需方签订协议，为其提供产品或服务的组织或个人。

注1：供方可能是承包商、生产方、供货商或零售商。

注2：在某些情形下，供方和需方属于同一组织。

[ISO/IEC 12207:2008]

4.1.17

测试（活动）　test

在规定的条件下执行系统或组件、对结果进行观察或记录，并就该系统或该组件的某些方面作出评价的活动。

[IEEE std 610.12—1998]

4.1.18

测试用例　test case

为某个特定目标（例如，为演练具体的程序路径或验证对特定需求的依从性）而开发的输入、执行条件以及预期结果的集合。

[IEEE std 610.12—1998]

4.1.19

测试文档集　test documentation

测试活动特有的文档汇集。

4.1.20

测试目标　test objective

待测量的已标识的软件特征的集合，通过在规定的条件下将实际的行为与要求的行为进行比较而测量。

注：改写 IEEE std 610.12—1998。

4.1.21

测试计划　test plan

说明预期的测试活动的范围、途径、资源和进度的文档。

注：改写 IEEE std 610.12—1998。

4.1.22

测试规程　test procedure

对于给定测试用例的设置、执行和结果评价的详细说明。

[IEEE std 610.12—1998]

4.1.23

测试（过程）　testing

在规定的条件下运行某一系统或组件，观察或记录其结果，并就该系统或组件的某些方面作出评价的过程。

[IEEE std 610.12—1998]

4.1.24

测试说明　testing description

测试执行条件的说明(即测试规程)。

4.1.25

用户　user

使用 RUSP 并获得收益的组织或个人。

注:在同一人或组织中,用户角色和操作员角色可能被同时赋予或先后赋予。

[ISO/IEC 12207:2008]

4.1.26

用户文档集　user documentation

随同软件提供的协助用户使用该软件的信息。

4.2 缩略语

下列缩略语适用于本文件。

CM:配置管理(Configuration Management)

RUSP:就绪可用软件产品(Ready to Use Software Product)

SQA:软件质量保证(Software Quality Assurance)

SQC:软件质量控制(Software Quality Control)

5 RUSP 的要求

5.1 产品说明要求

注:在 ISO/IEC 9127《软件工程　用于顾客软件包的用户文档集和封面信息》中有关封面信息的段落可用作编制产品说明的输入。

5.1.1 可用性

产品说明对于该产品的潜在需方和用户应是可用的。

5.1.2 内容

5.1.2.1　产品说明中宜阐明所运行软件的质量特性。

5.1.2.2　产品说明应包含潜在需方所需的信息,以便评价该软件对其需要的适用性。

5.1.2.3　产品说明应避免内部的不一致。

5.1.2.4　产品说明中包括的特性陈述应是可测试的或可验证的。

5.1.3 标识和标示

5.1.3.1　产品说明应显示唯一的标识。

5.1.3.2　RUSP 应以其产品标识指称。

5.1.3.3　产品说明应包含供方和(当适用时)供货商、电子商务供货商或零售商的名称和邮政或网络地址。

5.1.3.4　产品说明应标识该软件能完成的预期的工作任务和服务。

5.1.3.5　当供方想要声称符合有影响到该 RUSP 的法律或行政机构规定的文件时,则产品说明应标识出这些需求文档。

5.1.3.6　产品说明应陈述是否对运行 RUSP 提供支持。

5.1.3.7　产品说明应陈述是否提供维护。如果提供维护,则产品说明应陈述所提供的维护服务。

5.1.4 映射

产品说明中所提及的全部功能，宜按照软件产品质量特性的说明进行归类(5.1.5～5.1.12)。

5.1.5 产品质量——功能性

5.1.5.1 适用时，产品说明应根据 GB/T 25000.10—2016 包含有关功能性的陈述，要考虑功能完备性、功能正确性、功能适合性以及功能性的依从性，并以书面形式展示可验证的依从性证据。

5.1.5.2 产品说明应提供该产品中最终用户可调用的功能的概述。

5.1.5.3 产品说明应描述用户可能遭遇关键缺陷的所有功能。

注 1：关键缺陷可能是：

——数据丢失；

——死锁。

注 2：更多的信息参见 ISO/IEC 15026。

5.1.5.4 产品说明应给出用户可能碰到的所有已知的限制。

注：这些限制可能是：

——最小或最大值；

——密钥长度；

——一个文件中记录的最大数目；

——搜索准则的最大数目；

——最小样本规模。

5.1.5.5 当有软件组件的选项和版本时，应无歧义地予以指明。

5.1.5.6 当提供对软件的未授权访问(不管是无意的还是故意的)的预防措施时，则产品说明应包含这种信息。

5.1.6 产品质量——性能效率

5.1.6.1 适用时，产品说明应根据 GB/T 25000.10—2016 包含有关性能效率的陈述，要考虑时间特性、资源利用性、容量以及性能效率的依从性，并以书面形式展示可验证的依从性证据。

5.1.6.2 所有已知的影响性能效率的条件都应说明。

注：所陈述的条件可能是：

——系统配置；

——RUSP 有效工作所需的资源，例如带宽、硬盘空间、随机存储器、视频卡、无线互联网卡、CPU 速度等。

5.1.6.3 产品说明中应描述系统的容量，尤其与计算机系统相关的容量。

5.1.7 产品质量——兼容性

5.1.7.1 适用时，产品说明应根据 GB/T 25000.10—2016 包含有关兼容性的陈述，要考虑共存性、互操作性以及兼容性的依从性，并以书面形式展示可验证的依从性证据。

5.1.7.2 产品说明应以适当的引用文档指明 RUSP 在何处依赖于特定软件和(或)硬件。

5.1.7.3 产品说明应标识用户调用的接口和相关的被调用软件。

5.1.8 产品质量——易用性

5.1.8.1 适用时，产品说明应根据 GB/T 25000.10—2016 包含有关易用性的陈述，要考虑可辨识性、易学性、易操作性、用户差错防御性、用户界面舒适性、易访问性以及易用性的依从性，并以书面形式展示可验证的依从性证据。

5.1.8.2 产品说明应指明用户接口的类型。

注：这些接口可能是：

——命令行；

——菜单；

——视窗；
——功能键。

5.1.8.3 产品说明应指明使用和操作该软件所要求的专门知识。

注：这些专门知识可能是：
——所使用的数据库调用和协议的知识；
——技术领域的知识；
——操作系统的知识；
——经专门培训可获得的知识；
——产品说明中已写明的语言之外的其他语言的知识。

5.1.8.4 如适用，产品说明应描述防止用户误操作的功能。

5.1.8.5 当预防版权侵犯的技术保护妨碍易用性时，则应陈述这种保护。

注：这些保护可以是：
——程序设置的使用截止日期；
——拷贝付费的交互式提醒。

5.1.8.6 产品说明应包括可访问性的规定标示，特别是对有残疾的用户和存在语言差异的用户。

5.1.9 产品质量——可靠性

5.1.9.1 适用时，产品说明应根据 GB/T 25000.10—2016 包含有关可靠性的陈述，要考虑成熟性、可用性、容错性、易恢复性以及可靠性的依从性，并以书面形式展示可验证的依从性证据。

注：除非开发者能以服务数据或其他可验证的数据证实所做的声称，否则开发者不宜作出可靠性声称。

5.1.9.2 产品说明应就软件在遇到由用户接口出错、应用程序自身的逻辑出错、系统或网络资源可用性引发差错的情况下的继续运行(即可用)能力作出说明。

5.1.9.3 产品说明应包括关于数据保存和恢复规程的信息。

注：指明数据备份由操作系统的功能来执行也是可接受的。

5.1.10 产品质量——信息安全性

适用时，产品说明应根据 GB/T 25000.10—2016 包含有关信息安全性的陈述，要考虑保密性、完整性、抗抵赖性、可核查性、真实性以及信息安全性的依从性，并以书面形式展示可验证的依从性证据。

5.1.11 产品质量——维护性

5.1.11.1 适用时，产品说明应根据 GB/T 25000.10—2016 包含有关维护性的陈述，要考虑模块化、可重用性、易分析性、易修改性、易测试性以及维护性的依从性，并以书面形式展示可验证的依从性证据。

5.1.11.2 产品说明应包括用户所需的维护信息。

注：这些信息可能是：
——监控应用程序的动态性能信息；
——监控意外失效和重要条件的信息；
——监控运行指示器(如日志、警告屏)的信息；
——监控由应用程序处理本地数据的信息。

5.1.11.3 当该软件能由用户作修改时，则应标识用于修改的工具或规程及其使用条件。

注：使用的条件可能是：
——参数的变更；
——计算算法的变更；
——接口定制；
——功能键指派。

5.1.12 产品质量——可移植性

5.1.12.1 适用时，产品说明应根据 GB/T 25000.10—2016 包含有关可移植性的陈述，要考虑适应性、易安装性、易替换性以及可移植性的依从性，并以书面形式展示可验证的依从性证据。

5.1.12.2 产品说明应指明将该软件投入使用的不同配置或所支持的配置(硬件,软件)。

注1:针对不同工作任务、不同的边界值或不同的效率要求,可以规定不同配置。

注2:这些系统可能是:

——操作系统;
——包括协处理器的处理器;
——主内存规模;
——外存的类型和规模;
——扩展卡;
——输入和输出设备;
——网络环境;
——系统软件和其他软件。

5.1.12.3 产品说明应提供安装规程信息。

5.1.13 使用质量——有效性

5.1.13.1 适用时,产品说明应根据 GB/T 25000.10—2016 包含有关使用质量中有效性的陈述。

5.1.13.2 产品说明应对用户指明为实现特定目标产品所遵循的任何依从性基准。

5.1.14 使用质量——效率

5.1.14.1 适用时,产品说明应根据 GB/T 25000.10—2016 包含有关使用质量中效率的陈述。

5.1.14.2 产品说明应指明该 RUSP 预定是在单一系统上供多个并发最终用户使用,还是供一个最终用户使用,并且应说明在所要求的系统的所陈述的性能级别上可行的最大并发最终用户数。

5.1.14.3 产品说明应说明用户实现特定目标所需的资源信息。

5.1.15 使用质量——满意度

5.1.15.1 适用时,产品说明应根据 GB/T 25000.10—2016 包含有关使用质量中满意度的陈述,要考虑有用性、可信性、愉悦性和舒适性。

5.1.15.2 产品说明中应提供供方的联系方式,以便用户为了满意地使用该产品而联系他们。

5.1.16 使用质量——抗风险

5.1.16.1 适用时,产品说明应根据 GB/T 25000.10—2016 包含有关使用质量中抗风险的陈述,要考虑经济风险缓解性、健康和安全风险缓解性和环境风险缓解性。

5.1.16.2 在软件的使用存在已知的风险或需要特殊培训的情况下,产品说明中应包括非公开信息。

5.1.17 使用质量——周境覆盖

5.1.17.1 适用时,产品说明应根据 GB/T 25000.10—2016 包含有关使用质量中周境覆盖的陈述,要考虑周境完备性和灵活性。

5.1.17.2 如果产品说明中包含依从性的信息,该依从性的覆盖范围应明确说明。

5.2 用户文档集要求

注:ISO/IEC 9127《软件工程　用于顾客软件包的用户文档集和封面信息》有关封面信息的段落可以用于创建用户文档集。

5.2.1 可用性

用户文档集对于该产品的用户应是可用的。

5.2.2 内容

用户文档集包括的功能应是可测试的或可验证的。

5.2.3 标识和标示

5.2.3.1 用户文档集应显示唯一的标识。
5.2.3.2 RUSP 应以其产品标识指称。
5.2.3.3 用户文档集应包含供方的名称和邮政或网络地址。
5.2.3.4 用户文档集应标识该软件能完成的预期工作任务和服务。

5.2.4 完备性

5.2.4.1 用户文档集应包含使用该软件必需的信息。
5.2.4.2 用户文档集应说明在产品说明中陈述的所有功能以及最终用户能调用的所有功能。
5.2.4.3 用户文档集应列出已处理处置、会引起应用系统失效或终止的差错和缺陷，特别是列出那些最终导致数据丢失的应用系统终止的情况。
5.2.4.4 用户文档集应给出必要数据的备份和恢复指南。
5.2.4.5 对于所有关键的软件功能(即失效后会对安全产生影响或会造成重大财产损失或社会损失的软件)，用户文档集应提供完备的指导信息和参考信息。

注：更多信息参见附录 A。

5.2.4.6 用户文档集应陈述安装所要求的最小磁盘空间。
5.2.4.7 对用户要执行的应用管理职能，用户文档集应包括所有必要的信息。

注：信息示例——让用户能验证是否成功执行应用管理职能的信息。

5.2.4.8 如果用户文档集分若干部分提供，在该集合中至少有一处应标识出所有的部分。

5.2.5 正确性

5.2.5.1 用户文档集中的所有信息对主要的目标用户应是恰当的。

注：用户文档集中的所有信息的正确性都宜追溯到权威来源。

5.2.5.2 用户文档集不应有歧义的信息。

5.2.6 一致性

用户文档集中的各文档不应自相矛盾、互相矛盾以及与产品说明矛盾。

5.2.7 易理解性

5.2.7.1 用户文档集应采用该软件特定读者可理解的术语和文体，使其容易被 RUSP 主要针对的最终用户群理解。
5.2.7.2 应通过经编排的文档清单为理解用户文档集提供便利。

5.2.8 产品质量——功能性

用户文档集中应陈述产品说明中所列的所有限制。

5.2.9 产品质量——兼容性

5.2.9.1 用户文档集中应提供必要的信息以标识使用该软件的兼容性要求。
5.2.9.2 用户文档集应以适当的引用文档指明 RUSP 在何处依赖于特定软件和(或)硬件。

注：这种引用可包括：

——软件和(或)硬件的名称；

——版本；

——特定操作系统。

5.2.9.3 当用户文档集引证已知的、用户可调用的与其他软件的接口时，则应标识出这些接口或软件。

5.2.10 产品质量——易用性/易学性

用户文档集应为用户学会如何使用该软件提供必要的信息。

注：用户文档集可引用 RUSP 自身包含的或诸如培训之类辅助材料中包含的附加信息。

5.2.11 产品质量——易用性/易操作性

5.2.11.1 如果用户文档集不以印刷的形式提供，则文档集应指明是否可以被打印，如果可以打印，那么指出如何获得打印件。

5.2.11.2 卡片和快速参考指南以外的用户文档集，应给出目次（或主题词列表）和索引。

5.2.11.3 用户文档集应对所用到的术语和缩略语加以定义，以便用户可以理解文档中的用词。

5.2.12 产品质量——可靠性

用户文档集应描述可靠性的特征及其操作。

5.2.13 产品质量——信息安全性

用户文档集应对用户管理的每一项数据所对应的软件信息安全级别给出必要的信息。

5.2.14 产品质量——维护性

用户文档集应陈述是否提供维护。如果提供维护，则用户文档应陈述和软件发布计划相应的维护服务。

5.2.15 使用质量——有效性

用户文档集应能帮助用户达到产品说明陈述的使用质量有效性的目标。

5.2.16 使用质量——效率

用户文档集应能帮助用户达到产品说明陈述的使用质量效率的目标。

5.2.17 使用质量——满意度

5.2.17.1 用户文档集应能帮助用户达到产品说明陈述的使用质量满意度的目标。

5.2.17.2 用户文档集应提供供方的联系方式，以便用户反馈满意度信息。

5.2.18 使用质量——抗风险

用户文档集应能帮助用户达到产品说明陈述的使用质量抗风险的目标。

5.2.19 使用质量——周境覆盖

用户文档集应能帮助用户达到产品说明中陈述的使用质量周境覆盖的目标。

5.3 软件质量要求

5.3.1 产品质量——功能性

5.3.1.1 安装之后，软件的功能是否能执行应是可识别的。

注：对功能良好的验证可通过如下方式进行：利用所提供的测试用例，或按相应的消息自测试，或由用户进行的其他测试。

5.3.1.2 在给定的限制范围内，使用相应的环境设施、器材和数据，用户文档集中所陈述的所有功能应是可执行的。

5.3.1.3 软件应符合产品说明所引用的任何需求文档中的全部要求。

5.3.1.4　软件不应自相矛盾，并且不与产品说明和用户文档集矛盾。

注：两种完全相同的动作将产生同样的结果。

5.3.1.5　由遵循用户文档集的最终用户对软件运行进行的控制与软件的行为应是一致的。

5.3.2　产品质量——性能效率

软件应符合产品说明中有关性能效率的陈述。

注：当等待响应的时间不合理时向最终用户发送消息。

5.3.3　产品质量——兼容性

5.3.3.1　如果用户可以进行安装操作，则软件应提供一种方式来控制已安装组件的兼容性。

5.3.3.2　软件应按照用户文档集和产品说明中所定义的兼容性特征来执行。

5.3.3.3　如果软件需要提前配置环境和参数，以执行已定义的兼容性，应在用户文档集中明确说明。

5.3.3.4　在用户文档集中应明确指明兼容性、功能、数据或流的类型。

5.3.3.5　软件应能识别出哪个组件负责兼容性。

5.3.3.6　如果用户可以进行安装操作，且软件在安装时对组件有共存性的约束条件，则在安装前应予以明示。

5.3.4　产品质量——易用性

5.3.4.1　用户在看到产品说明或者第一次使用软件后，应能确认产品或系统是否符合其需要。

5.3.4.2　有关软件执行的各种问题、消息和结果都应是易理解的。

注1：借助以下的手段可以达到易理解性：

——恰当地选择术语；

——图形表示；

——提供背景信息；

——由帮助功能解释；

——提供易理解的文字或图形输出；

——提供清晰的音频输出。

注2：关于易用性问题，鼓励依据本部分达成协定的各方调查应用 ISO 9241 系列标准最新版本的可能性。特别是宜考虑 ISO/IEC 9241 系列标准的第 1、2、10 至 17 部分及 GB/T 25000.62《软件工程　软件产品质量要求和评价(SQuaRE)　易用性测试报告行业通用格式(CIF)》。

5.3.4.3　每个软件出错消息应指明如何改正差错或向谁报告差错。

注：这种信息可以是对用户文档集中某一项的引用。

5.3.4.4　出自软件的消息应设计成使最终用户易于理解的形式。

注：这些消息可能是：

——确认；

——软件发出的询问；

——信息；

——警告；

——出错消息。

5.3.4.5　屏幕输入格式、报表和其他输出对用户来说应是清晰且易理解的。

5.3.4.6　对具有严重后果的功能执行应是可撤销的，或者软件应给出这种后果的明显警告，并且在这种命令执行前要求确认。

注：数据的删除和盖写以及中断一个很长的处理操作均具有严重的后果。

5.3.4.7　借助用户接口、帮助功能或用户文档集提供的手段，最终用户应能够学习如何使用某一功能。

5.3.4.8　当执行某一功能时，若响应时间超出通常预期限度，应告知最终用户。

5.3.4.9　每一元素(数据媒体、文件等)均应带有产品标识，如果有两种以上的元素，则应附上标识号或标识文字。

5.3.4.10　用户界面应能使用户感觉愉悦和满意。

5.3.5 产品质量——可靠性

5.3.5.1 软件应按照用户文档集中定义的可靠性特征来执行。

5.3.5.2 与差错处置相关的功能应与产品说明和用户文档集中的陈述一致。

注：软件不能承担源自操作系统或网络的各种失效的责任。

5.3.5.3 在用户文档集陈述的限制范围内使用时，软件不应丢失数据。

注：这种要求即使在下面的情况下也要满足：

——利用的容量达到规定的极限；

——试图利用超出规定极限的容量；

——由产品说明中列出的其他软件或由最终用户所造成的不正确输入；

——违背用户文档集中明示的细则。

5.3.5.4 软件应识别违反句法条件的输入，并且不应作为许可的输入加以处理。

5.3.5.5 软件应具有从致命性错误中恢复的能力，并对用户是明显易懂的。

5.3.6 产品质量——信息安全性

5.3.6.1 软件应按照用户文档集中定义的信息安全性特征来运行。

5.3.6.2 软件应能防止对程序和数据的未授权访问(不管是无意的还是故意的)。

5.3.6.3 软件应能识别出对结构数据库或文件完整性产生损害的事件，且能阻止该事件，并通报给授权用户。

5.3.6.4 软件应能按照信息安全要求，对访问权限进行管理。

5.3.6.5 软件应能对保密数据进行保护，只允许授权用户访问。

5.3.7 产品质量——维护性

5.3.7.1 软件应按照用户文档集中定义的维护性特征来执行。

注：例如缺陷诊断的能力，使能修改的能力。

5.3.7.2 软件应能识别出每一个基本组件的发布号、相关的质量特性、参数和数据模型。

5.3.7.3 软件应能在任何时候都识别出每一个基本组件的发布号，包括安装的版本，以及对软件特征产生的影响。

注：基本组件可能是：

——数据屏幕；

——数据库模型；

——子程序；

——接口。

5.3.8 产品质量——可移植性

5.3.8.1 如果用户能够实施安装，遵循安装文档中的信息应能成功地安装软件。

5.3.8.2 对于软件应用程序的成功安装和正确运行，应就产品说明中列出的所有支持平台和系统加以证实。

5.3.8.3 软件应向用户提供移去或卸载所有已安装的组件的方法。

5.3.9 使用质量——有效性

5.3.9.1 软件应按照产品说明中陈述的使用质量——有效性特征来执行并通过用户文档获得帮助。

5.3.9.2 软件应能提供评价其对期望的依从性目标的影响的手段。

5.3.10 使用质量——效率

5.3.10.1 软件应按照产品说明中陈述的使用质量——效率特征来执行并通过用户文档获得帮助。

5.3.10.2 软件应能提供评价其在须达到目标时的使用效率的手段。

5.3.11 使用质量——满意度

5.3.11.1 软件应按照产品说明中陈述的使用质量——满意度特征来执行并通过用户文档获得帮助。
5.3.11.2 维护合同生效后，软件应提供直接与供方进行联络的途径。

5.3.12 使用质量——抗风险

5.3.12.1 软件应按照产品说明中陈述的使用质量——抗风险特征来执行并通过用户文档获得帮助。
5.3.12.2 对于所有有风险的功能，软件应提供特定的确认过程和管理权限。
5.3.12.3 对于所有有风险的功能，软件应有审计追踪。

5.3.13 使用质量——周境覆盖

5.3.13.1 软件应按照产品说明中陈述的使用质量——周境覆盖特征来执行并通过用户文档获得帮助。
5.3.13.2 如果软件使用参数限制功能性覆盖，用户应了解当前使用的功能的覆盖情况。

6 测试文档集要求

6.1 一般要求

6.1.1 目的

测试文档集的目的是证实软件与5.3中规定的要求的符合性。其中包含允许作这种证实的全部元素。

6.1.2 一致性

6.1.2.1 测试文档集中的每个文档所包含的信息应是正确的并且是可验证的。
6.1.2.2 测试文档集中的每个文档不应自相矛盾，并且不应与产品说明和用户文档集矛盾。

6.1.3 内容要求

6.1.3.1 测试文档集一般应包含：
a) 测试计划；
b) 测试说明；
c) 测试结果(报告)。

6.1.3.2 测试文档集应包含组成该汇集的全部文档的清单，清单中应包含全部文档的标题及其标识符。
6.1.3.3 测试文档集中的每个文档都应包括：
——标题；
——产品标识；
——修改历史，或说明该文档演变的任何其他元素；
——目次或对内容的说明；
——该文档正文中引用的文档的标识符；
——有关作者和审查者的信息；
——术语表。

6.1.3.4 测试文档集可由一个文档或多个文档组成。

6.1.4 方法

注：未推荐特定的技术或方法。

6.1.4.1 在产品说明和5.3软件质量要求中提及的所有质量特性均应经测试用例测试。
6.1.4.2 在产品说明和5.3软件质量要求中提及的每个质量特性至少应经一个测试用例测试。

注：测试计划可引用任何其他文档，前提是被引用的文档与用户文档集之间存在某种关系。

6.1.4.3 用户文档集中说明的所有功能，以及待完成的任务的代表性的功能组合，均应经测试用例测试。

6.1.4.4 用户文档集说明的每个功能至少应经一个测试用例测试。

6.1.4.5 测试用例应能证实软件与用户文档集中的陈述的符合性。

6.1.4.6 当产品说明中提及需求文档时，所涉及的内容应经测试用例测试。

6.1.4.7 应指明选作测试用例设计基础的功能分解层次。

注：功能可能是：

——用户文档中的一段；

——一个 Shell 命令；

——人机界面的按钮；

——语言命令。

6.1.4.8 应指明测试用例的设计方法。

注：可能的设计方法有：

——边界值分析；

——检查表；

——数据流分析；

——故障插入；

——容量测试。

6.1.4.9 所有安装规程均应经测试用例测试。

6.1.4.10 在产品说明和用户文档集中指明的所有操作限制均应经测试用例测试。

6.1.4.11 对所标识的违反句法条件的输入应经测试用例测试。

6.1.4.12 如果用户文档集中给出若干示例，这些示例应用作测试用例，但整个测试不应局限于这些示例。

6.1.4.13 当 5.3 软件质量要求中的任何要求不适用时，应说明理由。

6.1.4.14 应对产品说明和用户文档集中所陈述的所有配置进行测试。

6.2 测试计划要求

6.2.1 通过——失败准则

测试计划应指明用于判定测试结果是否证实软件与产品说明和用户文档集的符合性准则。

6.2.2 测试环境

测试计划应规定将要进行的测试所处的软件测试环境。

注：可采用配置等效性证实。

6.2.3 进度

测试计划应规定每个测试活动和测试里程碑的进度。

注：测试活动可能有：

——测试环境搭建；

——测试文档编制；

——测试执行。

6.2.4 风险

6.2.4.1 测试计划应识别、更新并记录测试活动中存在的风险，并提供应对措施。

6.2.5 人力资源

测试计划中应明确每个测试活动所需的人力资源情况。

6.2.6 工具和环境资源

6.2.6.1 测试计划中应明确执行测试活动所需的工具。

6.2.6.2 如果使用特殊的工具和环境，测试计划中应说明选择这些工具和环境的原因以及预期的结果。

6.2.7 沟通

测试计划中应规定沟通机制和方式，以便在利益相关方之间共享测试文档和测试项。

6.3 测试说明要求

6.3.1 测试用例说明

6.3.1.1 对每个测试用例的说明应包括：

a) 测试目标；
b) 唯一性标识符；
c) 测试的输入数据和测试边界；
d) 详细实施步骤；
e) 系统的预期行为；
f) 测试用例的预期输出；
g) 结果解释的准则；
h) 用于判定测试用例的肯定或否定结果的准则；
i) 可陈述的对基于 GB/T 25000.10—2016 的质量特性的引用。

6.3.1.2 当有必要提供与测试计划中提供的信息相比对的补充信息时，应陈述环境及其他测试条件（详细的配置和初步工作）。

6.3.2 测试规程

6.3.2.1 测试规程应包括：

a) 测试准备；
b) 开始和执行测试所必需的动作；
c) 记录测试结果所必需的动作；
d) 停止和最终重新启动测试的条件和动作。

6.3.2.2 为提供测试的可重复性和可再现性，测试规程应足够详细。

6.3.2.3 在软件被纠正之后，对于所涉及的功能和任何相关的功能，应有一种重新测试的规程。

注： 说明测试规程可采用伪语言或命令语言。

6.4 测试结果要求

6.4.1 执行报告

6.4.1.1 执行报告应包括测试用例结果的全部汇总。

6.4.1.2 执行报告应证实已按测试计划执行了所有测试用例。

6.4.1.3 对于每个测试用例，执行报告均应包括以下内容：

a) 测试用例的标识符；
b) 测试执行日期；
c) 实施测试的人员姓名和职责；
d) 测试用例执行的结果；
e) 发现的异常清单；
f) 对于每一异常，要引用相应的异常情况报告；
g) 可陈述的对基于 GB/T 25000.10—2016 的质量特性的引用。

6.4.2 异常情况报告

6.4.2.1 异常情况报告应包括所发现的全部异常汇总。如果有的话,还应包括纠正情况和通过再测试的验证情况。

6.4.2.2 对于每个异常,异常情况报告的说明性部分应包括如下内容:

a) 异常的标识符;

b) 软件的标识符;

c) 对异常的说明;

d) 执行测试用例中异常发生点;

e) 异常的严重程度和可重现程度;

f) 可陈述的对基于 GB/T 25000.10—2016 的质量特性的引用。

注 1:异常的严重程度可以是“致命的”“严重的”“重大的”“微小的”“轻微的”。

注 2:可重现程度可以是“总是出现”“有时出现”“随机出现”“未尝试”“不可再现”“N/A”。

6.4.2.3 异常情况报告的纠正部分应论证发现的所有异常均已纠正,或者未纠正的原因。

6.4.2.4 异常情况报告的纠正部分对每个纠正项应包含如下内容:

a) 纠正项的标识符;

b) 纠正的日期;

c) 纠正者的姓名;

d) 对应于纠正项的修改标识符;

e) 纠正项的可能影响;

f) 纠正者可能有的评论。

6.4.2.5 异常情况报告中经重新测试验证的部分,应证实所有已纠正的功能都具有用户文档集中定义的行为。

6.4.2.6 异常情况报告中经重新测试验证的部分对每个验证项应包含如下内容:

a) 验证项的标识符;

b) 验证日期;

c) 验证者的姓名;

d) 用于验证的测试用例;

e) 验证的结果;

f) 可陈述的对基于 GB/T 25000.10—2016 的质量特性的引用。

6.4.3 测试结果的评估

关于执行报告和异常情况报告的评估应表明:在所使用的判定测试结果是否在该软件的符合性准则的界限内,所有的期望行为是可获得的。

7 符合性评价细则

7.1 一般原则

作为 RUSP 组成部分的产品说明、用户文档集以及所交付的软件,应就其与第 5 章的要求做符合性评价。

注:“符合性评价”这一术语并不隐含任何技术或工具:测试、确认、验证、评审、分析等。

这些细则主要针对符合性评价组织进行的评价。符合性评价组织可以是根据某种认证模式工作的测试实验室,或是独立于 RUSP 供方的内部测试实验室。

7.2 符合性评价先决条件

7.2.1 RUSP 项已存在

对于 RUSP 的评价，待交付的所有项(见 5.2.4.8)以及在产品说明中标识的需求文档(见 5.1.3.5)均应是可用的。

7.2.2 系统元素已存在

在产品说明中说明的所有计算机系统的所有组件均应存在，并是可供符合性评价使用的。

7.3 符合性评价活动

注：未推荐任何特定的技术或工具。

符合性评价方法宜在文档中予以明确。

7.3.1 产品说明符合性评价

实施符合性评价以确定产品说明与 5.1 的要求的符合性。

7.3.2 用户文档集符合性评价

实施符合性评价以确定用户文档集与 5.2 的要求的符合性。

7.3.3 软件符合性评价

通过产生符合第 6 章要求(不包括与纠正异常和重新测试验证相关的部分)的测试文档集(6.4.2.3～6.4.2.6)来实施符合性评价，以确定软件与 5.3 的要求的符合性。

注：测试文档集包括对发现的异常的说明部分，然而对所发现的异常的纠正超出符合性评价组织符合性评价的范围。

7.4 符合性评价过程

供方将 RUSP 提供给符合性评价组织。供方还可提供测试文档集。

当供方仅提供 RUSP 而没有提供测试文档时，符合性评价组织应：

a) 依据 7.3 的要求，对产品说明、用户文档集及软件实施符合性评价；

b) 依据 7.5 的要求，将结果记录在符合性评价报告中。

当供方提供 RUSP 和测试文档时，符合性评价组织应：

a) 依据 7.3.1 和 7.3.2 的要求，对产品说明和用户文档集实施符合性评价；

b) 依据第 6 章的要求，对测试文档实施符合性评价；

c) 依据 7.5 的要求，将结果记录在符合性评价报告中。

注 1：测试文档与第 6 章的要求的符合性确立了软件与 5.3 的要求的符合性。

注 2：在符合性评价过程中可以生成附加的测试文档。

7.5 符合性评价报告

符合性评价组织应编制符合性评价报告。

符合性评价报告应确立 RUSP 与第 5 章的要求的符合性。

符合性评价报告应包含以下各项：

a) RUSP 标识；

b) 执行评价的人员姓名；

c) 评价完成日期以及(若有时)测试完成日期；

d) 若有时，用于进行测试的计算机系统(硬件、软件及其配置)；

e) 使用的文档及其标识；

f) 符合性评价活动汇总以及(若有时)测试活动汇总；

g) 符合性评价结果汇总以及(若有时)测试结果汇总；

h) 符合性评价的详细结果以及(若有时)测试的详细结果；

i) 若有时，不符合要求项的清单。

符合性评价报告的结果部分[上述的 f)～h)]应包含产品说明和用户文档集的符合性评价结果。根据所提供的元素，它还应包含以下两项之一：

a) 在供方仅提供 RUSP 而未提供测试文档的情况下，应包含该软件相对于 5.3 的要求的测试结果，即异常情况报告(见 6.4.2.2)的说明性部分；

b) 在供方提供 RUSP 和测试文档的情况下，应包含测试文档与第 6 章的要求的符合性评价结果。

注：符合性评价报告仅包含异常情况报告的说明部分，因为纠正异常不是符合性评价组织的职责。

对纸质的符合性评价报告而言，符合性评价报告的标识(测试实验室、RUSP 标识、符合性评价报告日期)及其总页数均应出现在符合性评价报告的每一页上。

符合性评价报告应包括：

a) 效果声明：测试结果(若有时)和评价只与被测试和被评价的项有关；

b) 复制声明：除非以完整报告的形式复制，否则未经测试实验室书面批准不得部分复制符合性评价报告。

7.6 后续符合性评价

对已进行过符合性评价的 RUSP 再次进行评价时，要考虑前次的符合性评价。评价活动如下：

a) 文档和软件中的所有变更部分都应予以评价，视同新的 RUSP；

b) 预计要受到变更部分影响的，或受到所要求的系统的变更影响的所有未变更部分均应予以评价，视同新的 RUSP；

c) 其他所有部分至少进行抽样评价。

附 录 A
（资料性附录）
业务或安全攸关的应用系统中的 RUSP 的评价指南

A.1 综述

RUSP 常用于低风险应用系统，已经开发出来的许多 RUSP 并未考虑对安全、业务、法律，或对组织的目标的风险。在非攸关的应用系统中，RUSP 的软件功能如果不可操作或不正常工作，最坏情况是导致用户不满。在最坏的情况下，开发者必须通过修补缺陷、增删某些功能组件使之恢复，以满足用户反馈的要求。在许多类似的案例中，市场不要求严格的测试，能容忍带有某种程度缺陷的 RUSP。

然而，在使用 RUSP 对安全或业务风险确实产生了影响的情况下，如不能恰当地应用或测试 RUSP，其后果将是严重的。此种环境中的 RUSP 应用领域包括：航空、医疗设备、医药、空间与探险、电信、建筑、财务、升降机、铁路、防御系统等。空中和铁路交通管理、癌症患者放射剂量、税务和财务报表的订正等功能，都是系统内即使只有一个故障也会带来可怕后果的例子。这些系统的功能需求通过提供按适应广泛设计目标的各种硬件和软件体系结构得到满足。某些设计目标可以用硬件（例如专用集成电路和可编程逻辑器件）实现，而另一些设计目标用 RUSP 实现。

对于业务或安全攸关的应用系统，在评价其 RUSP 的应用时，RUSP 的用户最好既考虑产品和过程的属性，也要考虑应用的功能。

可由 RUSP 支持的软件设计目标可能包括 A.2～A.7 几个方面。

A.2 故障检测和包括软件冗余的故障容纳

故障检测是检查系统出错状态的过程。故障容纳技术可以辨识系统能够正确运行的“安全状态”。通过采用诊断程序，软件检查自身的和硬件的不正确的结果。诊断程序既可以定期运行，也可以作为后台进程持续运行。诊断程序可包括重复计算两次或更多次、奇偶检验以及循环冗余检验。采用冗余设计的关键函数，在各冗余组件之间采用表决来判定这些组件的正确性。[IEC 61508-7，11]

A.3 重试故障恢复

与通信相关的系统往往利用重试功能来进行故障后恢复，这种恢复技术在实时系统中不常用。系统监视其自身的故障，并将其重置到以前的安全状态继续运行。在与实时相关的系统中如果采用故障后恢复技术，则需要确保这种恢复能够在故障显露系统级错误之前完成。[IEC 61508-7，11]

A.4 多版本程序设计

在多版本程序设计中，各独立团队生成规定数目为 n 份的软件产品，即称为多版本软件。不过，对于要求安全状态的系统而言，只有 3 个版本是典型的，而其中的两个版本更胜任实现这种安全状态。软件产品的所有 n 个版本都是软件系统的组成部分。常常用不同的编程语言和算法来减少通用模式失效的出现。不过，由于不合适的顶层规格说明，通用模式差错仍然有出现的可能。在各版本之间可采用各种表决策略来选择哪一个版本更适合系统的要求。

A.5 恢复块程序设计

恢复块程序设计是独立编写的模块自检其正确性的一种技术。在 RUSP 中使用这种技术，需要将模块中的 RUSP 组件隔离，并在退出之前评估任何出错的结果。当模块检测出差错时，另一模块立即发挥作用，清除封装模块中 RUSP 的任何副作用并继续无差错操作。

A.6 模型跟随

模型跟随是一种技术，在这种技术中，RUSP 组件的基础模型存在于系统之中，并用来验证 RUSP 组件本身的正确操作。该模型能以多种技术表示，从简单的表查找到完整的模型表示，这依赖于待建模的 RUSP 功能的需求和复杂性。

A.7 封装程序

封装程序是用于保护、隔离或与另一个组件接口的软件层。封装程序是有活力的候选件，在不修改 RUSP 组件的条件下，保护系统免受 RUSP 组件的影响。封装程序能用来增强被包装的 RUSP 组件的体系，这使其能满足所有目标系统的要求。此外，封装程序还能用于掩蔽新的系统实现中尚未使用的 RUSP 的功能体系。

A.8 待考虑的确立 RUSP 质量特征的技术

表 A.1 提供验证技术列表，可用于评价高风险应用中 RUSP 的完整性。

表 A.1 高风险应用系统中 RUSP 导引

特征组件	目　的	可能的措施
存储保护	检查应用系统是否防止访问未得到授权的地址空间	进行测试，试图在指定的地址范围外执行、或进行读或写操作
栈溢出保护	检查 RUSP 是否提供防止栈溢出的设施	通过调用使栈溢出的功能进行测试。验证内核是否将任务挂起，或此任务是否将使整个系统搞垮
动态存储器分配额	检查 RUSP 是否具有资源保护机制以防恶性任务无限制地消耗资源	创建一项请求存储器无限循环的任务，而另一项任务要求的存储量很小。验证此临界任务不至于被 RUSP 搞垮
容错	验证内核能否恢复和记载故障出现前的事件	宜对 RUSP 的测试进行设计，以展示 RUSP 的基础特征组件是否能使系统设计者建立容错机制
同时中断和中断嵌套	确定系统为响应同时出现的两次中断所需时间	测量服务于高低两种优先级中断的潜伏时间。这种测试宜测量系统响应同时出现的两次中断所经历的时间。验证中断处置具有优先级处理
包含可选项或停止活动的代码	验证可选项或停止活动的代码选件的偶然执行	检查可使“闲”代码被激活的任何条件，然后测试此种条件

表 A.1（续）

特征组件	目　的	可能的措施
封装程序的使用	该封装程序是否保护了系统内的RUSP组件或掩蔽了不想要的功能	调查RUSP组件是否用于与原设计不同的应用周境
RUSP评价	确定RUSP特征组件的适宜性及其对系统设计的影响	机构内部的快速评价和(或)原型设计
RUSP获取计划	确定许可证、租约、维护协定、访问问题报告和访问源代码的潜在需要	管理部门与RUSP供方签署的计划
RUSP的CM/SQA计划	确定在机构内部和在RUSP供方现场的CM和SQA的由来和发展	管理部门与RUSP供方签署的CM/SQA计划。评审问题报告，确保对源代码和目标代码的实际版本控制
RUSP的SQC	依据RUSP进行的系统内和系统外测试	验证系统的每一个需求
RUSP集成计划	RUSP在系统内待配置的计划	专用集成软件。正确运行RUSP的专用HW平台(计时、划分、不期望的功能、死的或停止活动的代码的影响)
产品支持	确定产品支持的可用性	评价支持系统的充分性(帮助菜单、操作手册、产品说明、帮助桌面)
以前的认证与鉴定	RUSP(包括任何法规机构控制的产品)的服务史	确定RUSP的服务史是否包括任何高关键性应用，并调查在此种环境中的性能
使用质量	对使用的RUSP依从顾客和用户既定要求提供客观证据(基于测试和试验数据、数学建模和仿真)	对RUSP适合其目的并满足顾客和用户的要求所作的论证(通过数学建模和仿真)，进行验证和确认

附 录 B
（资料性附录）
如何使用本部分

本部分能以如下方式使用：

a） 对 RUSP 规格说明的有高级要求时，可采用第 5 章的“质量要求”作为输入，以便详化 RUSP 的规格说明；

b） 当要求测试软件作为 RUSP 的组成部分时：可根据第 6 章“测试文档集要求”中定义的要求详化测试文档；

c） 对于要证实 RUSP 的质量时，即证实与本部分的符合性时，可依据第 7 章进行符合性评价。然后，基于符合性评价报告作出认证或供方声明。

注：这 3 种可能的方式原则上是累加的，即一种情况只有在前面情况付诸实现后才能展开。

另外，附录 A 可用于业务或安全攸关的软件。

参 考 文 献

[1] GB/T 9386 计算机软件测试文档编制规范

[2] GB/T 11457—2006 信息技术 软件工程术语

[3] GB/T 15481—2000 检测和校准实验室能力的通用要求(idt ISO/IEC 17025:1999)

[4] GB/T 16260.2—2006 软件工程 产品质量 第2部分:外部度量(ISO/IEC TR 9126-2:2003,IDT)

[5] GB/T 16260.3—2006 软件工程 产品质量 第3部分:内部度量(ISO/IEC TR 9126-3:2003,IDT)

[6] GB/T 16260.4—2006 软件工程 产品质量 第4部分:使用质量的度量(ISO/IEC TR 9126-4:2004,IDT)

[7] ISO/IEC 导则 2:2004 标准化及相关的活动 一般词汇表

[8] ISO/IEC 17050-1:2004 符合性评定 供方的符合性声明 第1部分:一般要求

[9] ISO/IEC 17050-2:2004 符合性评定 供方的符合性声明 第2部分:支持文档

[10] ISO/IEC 9127 软件工程—顾客软件包的用户文档集和封面信息

[11] ISO/IEC 9241-1:1997 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第1部分:一般介绍

[12] ISO/IEC 9241-2:1992 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第2部分:任务要求指南

[13] ISO/IEC 9241-11:1998 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第11部分:易用性指南

[14] ISO/IEC 9241-12:1998 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第12部分:信息表示

[15] ISO/IEC 9241-13:1998 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第13部分:用户指南

[16] ISO/IEC 9241-14:1997 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第14部分:选单对话框

[17] ISO/IEC 9241-15:1997 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第15部分:命令对话框

[18] ISO/IEC 9241-16:1999 具有可视化显示终端(VDTs)的办公室工作的人类工效学要求 第16部分:直接操纵对话框

[19] ISO/IEC 12207:2008 系统与软件工程 软件生存周期过程

[20] ISO/IEC 15026 信息技术 系统与软件完整性级别

[21] ISO/IEC 25021 系统与软件工程 系统与软件产品质量要求和评价(SQuaRE) 质量测量元素

[22] ISO/IEC 25062 软件工程 软件产品质量要求和评价(SQuaRE) 易用性测试报告的通用行业格式

[23] IEEE Std 1044—2009 IEEE 标准 异常分类

GB/T 25000.51—2016

中 华 人 民 共 和 国
国 家 标 准
系统与软件工程　系统与软件质量要求和评价(SQuaRE)　第51部分:就绪可用软件产品(RUSP)的质量要求和测试细则
GB/T 25000.51—2016
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2016年11月第一版
*
书号:155066・1-55373

版权专有　侵权必究

GB/T 25000.51-2016